ABSTRACT

Disclosed is a method making it possible to detect and/or to avoid illicit modifications of manufacturer software within a GSM type system. The GSM type system includes a hard kernel and a soft kernel, a local data interface. If the signal received on the local data interface of the terminal is not valid, then the GSM terminal is placed in a disabled state. If the signal is a disconnection signal on the local data interface, or there is no signal, a secure startup procedure is instigated with execution of the control functions. The hard kernel is auto tested. If the auto test is OK, then the integrity of the soft kernel is tested. If this integrity is OK, then the terminal is activated for normal operation. If the integrity is KO, then the terminal is placed in a disabled state. If the auto test is KO, then the GSM terminal is placed in a disabled state. If the received signal is a valid startup signal. Then if the fuse is not blown, the GSM terminal is rendered enabled. If the fuse is blown, the terminal is rendered not totally enabled, by deactivating at least one of the enabled functions of the terminal. If the signal is a signal of JTAG test type, the test procedure is continued. If the signal is a test signal, start up is in nonsecure mode and the test procedure is continued.